I CLAIM:

1. In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said access points to a computer; and

operating said computer to compare format of said one or more received data packets to selected requirements of said protocol-specified format, and signaling an alert if said packets deviate from said protocol-specified format.

2. A method as specified in claim 1 wherein said protocol-specified format includes a header message portion and wherein said comparing of format comprises comparing format of said header message portion to said protocol-specified format.

3. A method as specified in claim 2 wherein said protocol is IEEE Standard 802.11.

4. A method as specified in claim 2 wherein said protocol is IEEE Standard 802.11 having a frame control field in said header message portion and wherein said comparing of format comprises comparing format of said frame control field.

5. A method as specified in claim 1 wherein said protocol is IEEE Standard 802.11, and further wherein said one or more received data packets comprise IEEE Standard 802.11 Management Frames.

6. A method as specified in claim 1 wherein said protocol is IEEE Standard 802.11, and further wherein said one or more received data packets comprise IEEE Standard 802.11 Control Frames.

7. A method as specified in claim 1 wherein said protocol is IEEE Standard 802.11, and further wherein said one or more received data packets comprise a first WEP flag.

8. A method as specified in claim 7 wherein said packets have a first WEP flag value which is inconsistent with a second WEP value stored in a state table on said computer.

9. A method as specified in claim 1 wherein said one or more received data packets comprise a first Protocol Version value which is inconsistent with a second Protocol Version value stored in a state table on said computer.

10. A method as specified in claim 1 wherein said one or more received data packets comprise a source MAC address which is a multicast address.

11. A method as specified in claim 1 wherein said one or more received data packets comprise a source MAC address which is a broadcast address.

12. A method as specified in claim 3 wherein said one or more received data packets comprise a first Power Management state variable which is inconsistent with a second Power Management state variable value stored in a state table on said computer.

13. A method as specified in claim 3 wherein the step of operating said computer further comprises checking a More Data field of said received data packets and further monitoring said access points for a possible denial of service attack.

14. A method as specified in claim 3 wherein said one or more received data packets comprise an unsupported Type value.

15. A method as specified in claim 3 wherein said one or more received data packets comprise an unsupported SubType value.

16. A method as specified in claim 1 wherein said one or more received data packets comprise a spoofed MAC address.

17. A method as specified in claim 3 wherein said one or more received data packets comprise a frame of length which is inconsistent with said protocol-specified format.

18. A method as specified in claim 1 further comprising the step of maintaining a state table in said computer.

19. In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said mobile units to a computer; and

operating said computer to compare format of said one or more received data packets to selected requirements of said protocol-specified format, and signaling an alert if said packets deviate from said protocol-specified format.

20. A method as specified in claim 19 wherein said protocol-specified format includes a header message portion and wherein said comparing of format comprises comparing format of said header message portion to said protocol-specified format.

21. A method as specified in claim 20 wherein said protocol is IEEE Standard 802.11 having a frame control field in said header message portion and wherein said comparing of format comprises comparing format of said frame control field.

22. A method as specified in claim 19 wherein said protocol is IEEE Standard 802.11, and further wherein said one or more received data packets comprise IEEE Standard 802.11 Management Frames.

23. A method as specified in claim 18 wherein said protocol is IEEE Standard 802.11, and further wherein said one or more received data packets comprise IEEE Standard 802.11 Control Frames.

24. A method as specified in claim 19 wherein said protocol is IEEE Standard 802.11.

25. A method as specified in claim 19 wherein said protocol is IEEE Standard 802.11, and further wherein said one or more received data packets comprise a first WEP flag.

26. A method as specified in claim 25 wherein said packets have a first WEP flag value which is inconsistent with a second WEP value stored in a state table on said computer.

27. A method as specified in claim 25 wherein said one or more received data packets comprise a first Protocol Version value which is inconsistent with a second Protocol Version value stored in a state table on said computer.

28. A method as specified in claim 24 wherein said one or more received data packets comprise a source MAC address which is a multicast address.

29. A method as specified in claim 24 wherein said one or more received data packets comprise a source MAC address which is a broadcast address.

30. A method as specified in claim 24 wherein said one or more received data packets comprise a first Power Management state variable which is inconsistent with a second Power Management state variable value stored in a state table on said computer.

31. A method as specified in claim 24 wherein the step of operating said computer further comprises checking a More Data field of said received data packets and further monitoring said access points for a possible denial of service attack.

32. A method as specified in claim 24 wherein said one or more received data packets comprise an unsupported Type value.

33. A method as specified in claim 24 wherein said one or more received data packets comprise an unsupported SubType value.

34. A method as specified in claim 24 wherein said one or more received data packets comprise a spoofed MAC address.

35. A method as specified in claim 24 wherein said one or more received data packets comprise a frame of length which is inconsistent with said protocol-specified format.

36. A method as specified in claim 1 further comprising the step of maintaining a state table in said computer.

37. In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said mobile units to a computer; and

operating said computer to compare selected portions of said one or more received data packets to values stored in a state table in accordance with a specified protocol, and signaling an alert if said selected portions of said one or more packets deviate from said values stored in said state table.

38. A method as specified in claim 37 wherein said specified protocol is IEEE Standard 802.11.

39. A method as specified in claim 37 further comprising the step of maintaining a state table in said computer.